Prepared Testimony of

Joseph Ansanelli

Chairman and CEO of Vontu, Inc.

March 15, 2005

2123 Rayburn House Office Building

Washington, D.C.

Before the United States House of Representatives

Subcommittee on Commerce, Trade, and Consumer Protection

"Protecting Consumer's Data: Policy Issues Raised by Choice Point"

Vontu, Inc. One California Street | Suite 1500 | San Francisco, CA 94111
415 364 8100 **TEL** 415 364 8190 **FAX** www.vontu.com **WEB**

Chairman Stearns, Ranking Member Schakowsky and all the Committee members, thank you for your ongoing focus on the protection of consumer data.

I am Joseph Ansanelli, CEO of Vontu, an information security solutions company that helps Fortune 500 organizations such as Best Buy, Prudential, Charles Schwab and others, prevent the loss of consumer data over the Internet. Given my experience with helping some of the largest companies in America protect their consumer data, I hope to provide a unique viewpoint on the question of policy considerations as a result of recent cases of consumer data loss and if there is a need for a national consumer data security standard.

Problem: Identity Theft Affects Millions Every Year

The FTC[1] estimated that in one year alone approximately 10 million people – or almost 5% of the US adult population - were victims of Identity Theft. These victims reported $5 billion in out-of-pocket expenses and countless hours of lost time repairing their credit histories. In the previous five years, almost 30 million people were victims of identity theft.

This is not only a problem for consumers, but for business as well. As part of the same FTC report, the losses to businesses totaled nearly $50 billion.

Additionally, there is a risk to companies that is not mitigated through insurance or other strategies – loss of consumer trust. Vontu commissioned a survey[2] of 1000 consumers in

---

[1] Federal Trade Commission – Identity Theft Survey Report, September, 2003

[2] Vontu Consumer Trust Survey, See Appendix 1

the United States to better understand the effect that security of customer data has on consumer trust and commerce. Some of the findings include:

- **Security drives purchasing decisions** – More than 75 percent of consumers said security and privacy were important in their decisions from whom they purchase.
- **Consumers will speak with their wallets** – Fifty percent said that they would move their business to another company if they did not have confidence in a company's ability to protect their personal data.
- **Insider theft increases concerns about a company's data security efforts** – More than 50 percent of the consumers surveyed said an insider breach would cause them to be more concerned about how a company secures their information

Clearly, financial costs and loss of consumer trust as a result of identity theft are a significant problem today.

Identity Theft Policy Implications

In order to reduce Identity Theft, there are at least three areas of focus for policy:

1. Criminals who steal identities. This is important not only for reducing Identity Theft, but other crimes and threats to national security. Professor Judith Collins of Michigan Statue University's ID Theft Crime Lab states that virtually all identity thieves are involved in other felonies or terrorist acts. The Identity Theft Penalty Enhancement Act, which became law in July 2004, was a positive step in the right direction to increase the penalties and provide additional tools for law enforcement and the courts to punish those found guilty of identity theft.
2. Consumers who need continued education on the importance of protecting their identities and as well as help if they are victims. The efforts of the FTC with the ID

Theft hotline, privacy website and on-going educational efforts are important and more can be done to raise awareness of those efforts. Additionally, the FACT Act provided much needed tools for consumers including free annual credit reports, the ability to place fraud alerts in their credit report, and ability to more easily correct inaccuracies in their credit report resulting from identity theft.

3. Organizations that store consumer data.

Responsibility of Organizations

The third area, companies, government agencies and organizations that store consumer data, is the one in which I have the most experience and is the focus of my testimony. An important point to understand, before we can truly begin to address the problem, is that these organizations are not the criminals perpetrating Identity Theft. In fact, all of the companies that I have worked with invest significant resources and are thoroughly committed in their efforts to protect consumer data.

However, we all recognize that organizations with consumer data are a crucial "link in the chain" to prevent identity theft and the question that many people are asking is:

"Are these organizations doing enough to ensure the security of consumer data?"

To answer that question, I suggest one must first ask:

"Is it clear to organizations what is expected of them to best protect consumer information?"

Unfortunately, despite existing legislation, there is confusion around what is required of organizations and confusion is the enemy of consumer protection.

Confusion is the Enemy of Consumer Protection

To date, Congress has taken important steps to address consumer information protection through industry and organization specific regulations. For example, Section 501 (b) of Gramm Leach Bliley for financial services, PART 164 - Subpart C of HIPAA for healthcare providers, the Driver's Privacy Protection Act for state DMVs, the Fair Credit Reporting and FACT Act, and others. Additionally, many states are creating de facto national requirements such as California SB 1386 which requires notification in the case of a breach.

These different legislative acts have aspects of consumer data protection yet each has tackled the problem differently based on industry or state specific requirements. And that is where the beginning of the confusion lies.

One important question for this committee to consider is:

"What is the difference in how a bank versus a retailer versus a utility provider should treat the security of a social security number, and should the focus of policy be on the industry of the data itself?"

National Consumer Data Security Standard

I am sure everyone would agree, it is the data that matters and needs to be protected across all industries. One possible solution to raise the level of consumer data protection is to extend existing industry specific consumer data protection requirements to cover *any* organization which stores private consumer data and create a preemptive and unified, National Consumer Data Security Standard.

One alternative would be very similar to GLBA and HIPAA[3] in addition to a requirement for notification. The difference is that it would apply to any organization that stores consumer information regardless of industry or location.

This standard would require any organization that stores non-public consumer data to:

1. Ensure the security and confidentiality of consumer information. This would create an affirmative obligation of the companies to protect the data.
2. Protect against any reasonably anticipated threats to the security of such information. This would allow the requirements to evolve as new threats emerge without new legislation.
3. Protect against unauthorized access to or use of such information that could result in substantial harm to a consumer. This would help prevent against fraudulent efforts to gain access to the data by outsiders or insiders as is the cause in many recent breaches.
4. Ensure compliance with their security policies by an organization's workforce and third parties who are given access to the information. This would address the issue of the insider threat, which was the situation in the recent Teledata case, as well as concerns regarding off shoring and outsourcing;
5. Disclose any loss of the information when it is reasonably believed that such loss could result in substantial harm to a consumer. This would help consumers to proactively protect themselves by monitoring their credit reports, setting up fraud alerts and other efforts to watch for potential issues.

---

[3] See attached Appendix 2 and 3

Rule making for this legislation would exist in relevant agencies and I believe that the FTC has already done much of the work under the GLBA Safeguards Rule 16 CFR Part 314 and could apply this rule beyond entities covered under GLBA.

In addition, while these requirements serve as the proverbial "stick", I suggest the Committee consider any new legislation also provide a "carrot" as an inventive to go beyond any base requirements. This "carrot" might provide some level of protection against excessive punitive damages for those organizations with qualifying security programs. This is important to help remove existing and valid concerns that organizations have about increased litigation risk as they proactively uncover new threats with respect to consumer data security. This is not protection against economic or reasonable pain and suffering damages, but against excessive punitive actions when companies are clearly meeting and exceeding these requirements.

Summary

In summary, to reduce identity theft policy must focus on the criminals, consumers and organizations that store the data.

I suggest this Committee consider the idea of a preemptive, national consumer data security standard that also protects organizations from potential excessive punitive damages when they are making best efforts to protect consumer information. The standard would clearly state what is required of an organization and encourage them to use their best efforts to improve the protection of consumer information and help to reduce Identity Theft.

Appendix 1: Relevant GLBA Section

Gramm Leach Blilely

TITLE V—PRIVACY

Subtitle A—Disclosure of Nonpublic Personal Information

SEC. 501. PROTECTION OF NONPUBLIC PERSONAL INFORMATION.

(b) FINANCIAL INSTITUTIONS SAFEGUARDS.— In furtherance of the policy in subsection (a), each agency or authority described in section 505(a) shall establish appropriate standards for the financial institutions subject to their jurisdiction relating to administrative, technical, and physical safeguards—

(1) to insure the security and confidentiality of customer records and information;

(2) to protect against any anticipated threats or hazards to the security or integrity of such records; and

(3) to protect against unauthorized access to or use of such records or information which could result in substantial harm or inconvenience to any customer.

Appendix 2: Relevant HIPAA Section

HIPAA Security Requirements

PART 164 - SECURITY AND PRIVACY

Subpart C Security Standards for the Protection of Electronic

Protected Health Information

Section 164.306 – *General requirements*

Covered entities must do the following:

(1) Ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity creates, receives, maintains, or transmits.
(2) Protect against any reasonably anticipated threats or hazards to the security or integrity of such information.
(3) Protect against any reasonably anticipated uses or disclosures of such information that are not permitted or required under subpart E of this part.
(4) Ensure compliance with this subpart by its workforce.

Attachment 1: 2003 Consumer Information Trust Survey

Attachment 2: Harris Interactive Database Security Highlights

Attachment 3: Ponemon Research on Data Security Breaches

Attachment 4: Vontu 2004 Data Security Trends Report

2003 Customer Information Trust Survey

Those organizations that sit on the highest perch when it comes to customer trust have the farthest to fall if they lose that trust according to the 2003 Customer Information Trust Survey commissioned by security technology innovator Vontu, Inc.

Consumers have the greatest amount of trust that companies within the health care industry have measures in place to protect personal information from identity thieves. Web retailers and retailers scored near the bottom in consumer trust in a ranking of 14 major industries. However, even the companies that scored well with consumers can face serious financial consequences if security breaches within their organization lead to a loss of consumer trust. Some of the major findings of the survey are:

- Security is important in the purchasing decision. More than 75 percent of the consumers said security and privacy was important in their decisions from whom they purchase.
- Not all security breaches are equal in the eye of the customer. More than 54 percent said security breaches by insiders or employees, now one of the fastest growing contributors to identity theft, would have the greatest impact on their trust in an organization.
- Consumers choose with their wallets. Fifty percent said that they would move their business to another company if they did not have confidence in a company's ability to protect their personal data.

Vontu Information Trust Rankings*

Hospital or Clinic 82%
Pharmacy 79%
Bank 78%
Charity/Religious Org. 78%
Airlines 60%
Car Rental Company 53%
Utility 48%
Credit Card Company 47%
Cable Company 42%
Restaurants 42%
Hotels 41%
Web Retailers 41%
Retail Stores 38%
Grocery Store 25%

* The Vontu Information Trust Rankings rate 14 major industries based on the level of trust consumers surveyed said they had that these organizations would protect personal information from identity theft.

Two examples of the questions from the survey are:

How important is privacy and security to your purchasing decision?

- Very important 19%
- Important 57%
- Not important 9%
- Unsure/No Comment 14%

If an insider (such as an employee of the company) stole your data rather than an outsider (such as a computer hacker), would it change your answers to previous question about trust?

- Yes – More concerned about insider 54%
- Yes – Less concerned about insider 12%
- No - No difference 17%
- Unsure/No comment 18%